



# ISO/IEC 42001:2023 para Infraestructura RAG e

Adaptación Operativa para Entornos On-Premise, Hardware Reacondicionado y Privacidad  
RGPD/EU AI Act

## 1. RESUMEN EJECUTIVO Y ALCANCE DEL SMIA

La implementación de soluciones de Inteligencia Artificial (IA) y Generación Aumentada por Recuperación (RAG) en las empresas exige garantizar un equilibrio estricto entre innovación operativa, soberanía de datos y cumplimiento normativo. El presente documento establece el marco de gobernanza bajo la norma internacional **ISO/IEC 42001:2023** (Sistema de Gestión de Inteligencia Artificial — SMIA), adaptado específicamente a una infraestructura **100% local (On-Premise)** basada en motor *Ollama*, interfaz y base vectorial *AnythingLLM / LanceDB* y hardware profesional reacondicionado de nivel empresarial.

**Pilar de Soberanía y Privacidad:** El procesamiento RAG en la propia red elimina las transferencias internacionales de datos y la exposición a APIs de terceros en la nube, garantizando el cumplimiento por diseño (*Privacy by Design*) exigido por la AEPD / RGPD y la Ley Europea de IA (*EU AI Act*).

## 2. ARQUITECTURA LOCAL Y EVALUACIÓN DE CRITICIDAD DEL RIESGO

El entorno RAG local procesa la información en cuatro fases secuenciales: Ingesta/Chunking (fragmentación de 300-1000 palabras), Vectorización mediante modelos ligeros de embeddings (*nomic-embed-text* o *bge-m3*), almacenamiento indexado en la base vectorial local *LanceDB*, e Inferencia conversacional utilizando LLMs optimizados de 7B/8B parámetros (*Llama 3*, *Mistral* o *Qwen 2.5*). El hardware soporta esta carga mediante estaciones reacondicionadas con 16 GB - 32 GB+ de RAM, GPUs dedicadas (NVIDIA RTX 3060/4070 o Apple Silicon) y almacenamiento SSD NVMe.

**Cálculo Matemático de Criticidad del Riesgo de IA (Cláusula 6.1.2 / ISO 42001):**

- $$C_{IA} = I_v \times M_{auto} \times E_{pop}$$
- $I_v$  (**Impacto de Vulnerabilidad**): Gravamen de una falla o alucinación del modelo (Escala 1 a 5).
  - $M_{auto}$  (**Nivel de Autonomía**): Grado de ausencia de supervisión humana (Escala 1 = Human-in-the-loop, 5 = Autónomo).
  - $E_{pop}$  (**Factor de Exposición**): Sensibilidad y volumen de datos/usuarios afectados (Escala 1 = Interno/Restringido, 5 = Público).

En el entorno RAG local implementado en modo Query y con supervisión humana,  $C_{IA}$  se mantiene en niveles Bajos-Moderados, garantizando un riesgo residual controlado.

## 3. MATRIZ DE CONTROLES ISO/IEC 42001 (ANNEXE A ADAPTADO)

La siguiente matriz especifica la aplicación de los **9 dominios temáticos del Anexo A (Controles A.2 a A.10)** adaptados a la infraestructura técnica local de la organización:



| Dominio                               | Objetivo de Control                                  | Implementación Técnica en IA Local                                                                                                                                     | Evidencia para Auditoría                                                     |
|---------------------------------------|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| A.2<br>Políticas de IA                | Alineación con la estrategia empresarial y ética.    | Publicación de la Política Interna de Uso Responsable de IA. Prohibición de envío de datos sensibles a LLMs en la nube sin autorización.                               | Política aprobada por la Dirección y registro de difusión a personal.        |
| A.3<br>Organización                   | Asignación clara de roles, autoridades y canales.    | Nombramiento del Responsable de Gobernanza del SMIA y establecimiento de canal interno de notificación de anomalías o alucinaciones.                                   | Matriz de roles (RACI) y registros del canal de incidencias.                 |
| A.4<br>Rendimiento y Recursos         | Evaluación de recursos humanos y computacionales.    | Suministro de hardware reacondicionado certificado (RAM 32GB, GPU VRAM 12GB, SSD NVMe). Formación en alfabetización en IA (AI Literacy).                               | Fichas de hardware, certificados de prueba y control de asistencia a cursos. |
| A.5<br>Evaluación de Impactos         | Análisis de impacto social, ético y de privacidad.   | Ejecución previa de la Evaluación de Impacto en la Protección de Datos (EIVP / PIA) según directrices de la AEPD antes del despliegue RAG.                             | Informe PIA documentado con matriz de riesgos y mitigaciones.                |
| A.6<br>Ciclo de Vida                  | Control desde la ingesta hasta el retiro de modelos. | Gestión del pipeline RAG: sanitización pre-ingesta, chunking estructurado, control de versiones del modelo (Ollama) y desmantelamiento seguro.                         | Procedimiento operativo estándar (SOP) e inventario de modelos.              |
| A.7<br>Gobernanza de Datos            | Calidad, representatividad y minimización de datos.  | Separación de datos por <i>Workspaces</i> independientes (Ventas, Legal). Transformación de hojas de cálculo complejas a Markdown narrativo para evitar sesgos.        | Estructura de workspaces y registros de sanitización/transformación.         |
| A.8<br>Transparencia y Explicabilidad | Información a partes interesadas y trazabilidad.     | Notificación explícita de interacción con IA. Generación obligatoria de citas y referencias hipervinculadas a páginas y documentos fuente.                             | Capturas del sistema RAG mostrando citas verificables y logs.                |
| A.9<br>Uso Responsable                | Mecanismos de supervisión humana permanente.         | Configuración en modo <i>Query</i> (respuesta estricta basada en documentos). Principio <i>Human-in-the-loop</i> : las decisiones finales requieren validación humana. | Configuración de AnythingLLM y registro de decisiones auditadas.             |
| A.10<br>Relación con Terceros         | Gobernanza de proveedores y modelos de terceros.     | Selección de socios de hardware reacondicionado con borrado seguro certificado de datos previa (NIST 800-88 / ISO 27001). Modelos open-weights verificados.            | Certificados de borrado de datos e inspección técnica de proveedores.        |

#### 4. PERFIL DE MITIGACIÓN DE RIESGOS Y CUMPLIMIENTO NORMATIVO

La transición de un modelo en la nube a un sistema RAG local acreditado bajo ISO 42001 genera una reducción drástica en la exposición a los principales riesgos de seguridad y cumplimiento legal:

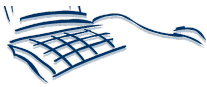
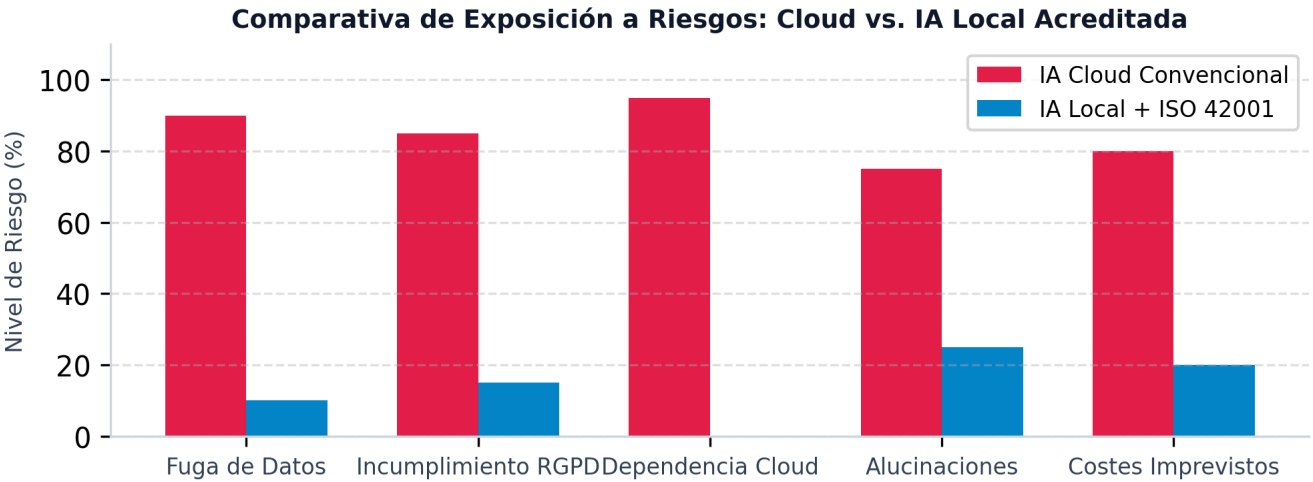


Figura 1: Reducción porcentual estimada de exposición a riesgos operativos y legales mediante IA Local On-Premise.

## 5. HOJA DE RUTA PARA LA CERTIFICACIÓN EXTERNA DEL SMIA

El proceso formal para obtener la certificación acreditada bajo ISO/IEC 42001:2023 consta de cinco fases principales:

|                                      |                                                                                                                                                              |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fase 1: Alcance y Gobernanza</b>  | Delimitación del contexto del SMIA (Cláusula 4), aprobación de la política de IA por la alta dirección y nombramiento del DPO/Responsable de IA.             |
| <b>Fase 2: Anexo A y SoA</b>         | Redacción de la Declaración de Aplicabilidad (SoA), formalización de la matriz de 38 controles y ejecución de la EIVP / PIA para la infraestructura RAG.     |
| <b>Fase 3: Operativo y Registros</b> | Despliegue del entorno Ollama + AnythingLLM en hardware reacondicionado, activación de logs de auditoría, control de accesos y programas de alfabetización.  |
| <b>Fase 4: Auditoría Interna</b>     | Ejecución de auditorías internas sistemáticas, evaluación de KPIs de rendimiento/desviación y revisión formal por la Dirección (Cláusulas 9 y 10).           |
| <b>Fase 5: Auditoría Externa</b>     | Evaluación formal por un organismo de certificación acreditado (Fase 1: Revisión documental; Fase 2: Evaluación in situ). Emisión del certificado ISO 42001. |

**Conclusión de Auditoría:** La combinación de hardware IT reacondicionado de alta gama con un entorno RAG local desconectado y la estructura de gobernanza ISO/IEC 42001 proporciona a la empresa una ventaja competitiva decisiva: máxima eficiencia financiera, soberanía absoluta sobre la propiedad intelectual y evidencia documental frente a inspecciones del RGPD o la Ley de IA de la UE.